

Customer Use of Microsoft Technology

One-third of professionally-managed assets incorporate sustainability criteria, representing \$17 trillion in investments.¹ More responsible fund dollars are invested in Microsoft than in any other single company.² The company secured its standing as a responsible business in part because it is committed to the environment, human rights, and democratic institutions. Microsoft advances the UN Sustainable Development Goals, established principles for responsible use of artificial intelligence ("AI"), and recognizes privacy as a "fundamental human right."³

Microsoft demands the same ethics in its supply chain: "When it comes to labor and human rights, we leave no doubt as to the standards we expect. Our standards apply to all our suppliers, including those at the farthest reaches of our supply chain."⁴ However, contrary to those standards, customers such as the Department of Defense, U.S. Army, and Department of Homeland Security appear to be using Microsoft's technology in ways that conflict with Microsoft's policies.

The government is weaponizing the company's technology, supplanting human decision-making with artificial intelligence, and using its products to gamify warfare and for surveillance, violating privacy, threatening civil rights, and circumventing legal requirements. These consequences tend to disproportionately impact people of color, activists and immigrants.

Three contracts serve as examples that raise concerns:

- Microsoft's HoloLens product recently moved from a prototype tested by the U.S. Army to a \$21 billion Integrated Visual Augmentation System ("IVAS") production contract for a military version to enable enhanced vision using AI-powered technology. The Army intends its close-combat lethality units to use IVAS in warfare to achieve "overmatch" against enemy forces.
- The Department of Defense awarded Microsoft a 10-year, \$10 billion contract for the Joint Enterprise Defense Infrastructure ("JEDI") for cloud services to assist with development of AI capabilities to operationalize warfare.
- Microsoft's contract with U.S. Immigration and Customs Enforcement ("ICE") provides law enforcement with access to personal information which, when matched with surveillance technology, has the potential to infringe on privacy and civil rights, and permits the agency to circumvent legal safeguards - such as search warrants - that normally serve as protection from government overreach.

¹ <https://www.ussif.org/files/Trends%20Report%202020%20Executive%20Summary.pdf> at p.5.

² <https://qz.com/1803716/microsoft-is-the-biggest-recipient-of-esg-rsi-stock-fund-investment/>

³ Microsoft's 2020 Corporate Social Responsibility Report at p.25.

⁴ *Id.* at p.16.

In addition to brand, reputational and financial risk, company employees have protested the conversion of their work-products to tools of war and surveillance. These concerns impact employee morale, risk internal productivity, and hamstringing recruitment efforts. Campaigns such as #NoTechForICE shed a bad light on Microsoft, and, as recently occurred with bank private prison funding, can quickly escalate into calls for divestment, (#RealMoneyMoves).

Whereas shareholders are concerned about potential harms to the company and society as set forth above, we urge shareholders to vote in favor of the following resolution:

Resolved, that the board commission an independent report to assess whether customer use of Microsoft's technology does or can contribute to violations of privacy, civil and human rights, and conflicts with the policies and principles set forth in Microsoft's CSR Report and other public disclosures.